Dated: February 2011
Approved: February 2011
Version: 0.93

	SOG-IS Recognition Agreement Management Committee Policies and Procedures

Document ID: SOGIS-IT-Technical-Domains-v0.93
Subject: IT-Technical Domains

General

1 This document will list the technical domains accepted by the Management Committee. This list will be updated by the Management Committee as required and supersedes the list of technical domains in Annex L from the SOGIS-MRA.

IT-Technical Domain "Smart card and similar devices"

Definition

2 This section provides the scope and rationale for the IT-Technical Domain "Smart card and similar devices".

3 This IT-Technical Domain is related to smart cards and similar devices where significant portions of the required security functionality depend upon hardware features at a chip level (for example smart card hardware/ICs, smart card composite products, TPMs used in Trusted Computing, digital tachograph cards, Hardware Security Modules, etc.).

Rationale

4 In the technologies covered by the scope above an attacker will often be able to obtain ready physical access to the device (or a set of devices), the device may well contain critical information such as security credentials/keys and part of the security functionality required of the device will relate to self protection either by active (tamper detection) or passive means (such as tamper resistant coatings). This contrasts with standard multipurpose hardware as used in a general processing equipment such as a PC.

5 The evaluation approach needs to consider all hardware specific aspects of vulnerability analysis including those that require significant additional equipment and resources. Such devices are frequently composed from elements produced by different developers (for example hardware, smart card operating system, and application) and may involve production across a range of development sites (e.g. IC design, mask production, fabrication, characterisation, etc). These factors must also be consistently taken into account during evaluation and certification.

List of approved JIWG supporting documents

6 The JIWG supporting documents listed in the following table support the evaluation of products related to the IT-Technical Domain ”Smart card and similar devices” up to EAL 7. They are continuously monitored and updated by the JIWG.

Title	Type
Application of CC to Integrated Circuits	Mandatory
Application of Attack Potential to Smartcards	Mandatory
Composite product evaluation for Smart Cards and similar devices	Mandatory
ETR for composite evaluation template	Guidance
Guidance for Smartcard evaluation	Guidance
Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices	Mandatory
Security Evaluation and Certification of Digital Tachographs	Mandatory
Attack Methods for Smartcards and Similar Devices	Mandatory
Requirements to perform Integrated Circuit Evaluations	Mandatory

IT-Technical Domain "Hardware Devices with Security Boxes"

Definition

7 This section provides the scope and rationale for the IT-Technical Domain "Hardware Devices with Security Boxes".

8 This IT-Technical Domain is related to products produced from a series of discrete parts on one or more printed circuit boards whereby significant proportions of the required security functionality depend upon a hardware physical envelope with counter-measures (a so-called "Security Box") against direct physical attacks (for example payment terminals, tachograph vehicle units, smart meters, taxi meters, access control terminals, Hardware Security Modules, etc.).

Rationale

9 In the technologies covered by the above scope, an attacker will often be able to obtain ready physical access to the device (or a set of devices). The device may well contain critical information such as security credentials/keys, or could be used also for secure entry of credentials/keys and a significant part of the security functionality required of the device will relate to self protection against physical attacks. These self protection counter-measures or the "security box" of such devices is composed of physical protection counter-measures based on hardware and software active mechanisms. Usually these mechanisms involves also passive protections as an inherent part of the provided security functionality e.g. metallic shields or armoured plating, wire meshing, chemical protections like epoxy resin, etc. in conjunction with sensors and electronic anti-tampering mechanisms like secure data erasing, alarm generation or component emergency destruction.

10 The evaluation approach needs to consider all software, firmware and hardware specific aspects of vulnerability analysis including those that may require significant additional equipment and resources. Such devices are also frequently composed from discrete parts produced by different developers. These factors must also be consistently taken into account during evaluation and certification.

List of approved JIWG supporting documents

11 The JIWG supporting documents listed in the following table support the evaluation of products related to the IT-Technical Domain "Hardware Devices with Security Boxes" up to EAL7. They are continuously monitored and updated by the JIWG.

Title	Type
ETR for risk management template	Draft
Guidance for POI evaluation	Draft
Application of Attack Potential to Hardware Devices with Security Boxes	Draft
Attack Methods for Hardware Devices with Security Boxes	Draft
Requirements to perform Hardware Devices with Security Boxes Evaluations	Draft